

SUIS: An Online Graphical Signature-Based User Identification System

Shahid Alam

Department of Computer Science and Engineering
Qatar University, Doha, Qatar
Email: salam@qu.edu.qa

Abstract—Humans possess a large amount of, and almost limitless, visual memory, that assists them to remember pictures far better than words. This phenomenon has recently motivated the computer security researchers' in academia and industry to design and develop graphical user identification systems (GUIs). *Cognometric* GUIs are more memorable than *drawmetric* GUIs, but takes more time to authenticate. None of the previously proposed GUIs combines the advantages of both *cognometric* and *drawmetric* systems. A signature personify a person and a graphical signature is easier to recall than other drawings. This paper proposes a new graphical Signature-based User Identification System named SUIS. It is based on a 2D grid technology, that is used to draw, digitize and store the signature for user identification. SUIS is categorized as both a *cognometric* and *drawmetric* system. Unlike other systems that use 2D grid: We take one cell in a grid as one pixel in the drawing; for signature matching, the signature drawn has to follow the same grid cells as the signature stored, independent of the sequence; and that the system is not based on any machine learning model. Increasing the number of grid cells increases the password space, and decreasing the size of the grid cell increases the precision of the signature. These characteristics makes SUIS: (1) Rigorous enough to be a password system, but easy enough to be usable. (2) Independent of the language and device used to draw the signature. (3) Efficient and practical to be used for online authentication systems.

I. INTRODUCTION AND MOTIVATION

The traditional methods for user identification systems rely on entering a username and a text password. One of the major vulnerabilities of this technique is the difficulty of remembering passwords. Therefore the users tend to pick short passwords or passwords that are easy to remember. These passwords can be easily broken. Passwords that are hard to break are often hard to remember.

The ability of humans to remember pictures far better than words [13, 14] has recently motivated computer security researchers' in academia [1, 6, 7, 8, 9, 10, 12, 18, 19, 21, 23] and industry [4, 5, 15, 16, 20, 22] to study, design and develop graphical user identification systems (GUIs). More than 10 US patents on GUIs have been issued, the first in 1996 to Greg E. Blonder [2] and the last in 2014 to Microsoft Corporation [11], but yet GUIs are not widely used.

There are three basic categories of GUIs [6]: *Cognometrics*, *Locimetrics*, and *Drawmetrics*. *Cognometric* systems are based on the human cognitive abilities, such as the ability to remember and recall images. *Locimetric* systems are based on locating or identifying a point in an image. *Drawmetric*

systems are based on reproducing an already pre-drawn image (outline drawing).

Elizabeth et al. [17] presents a study about the relationship between memory and graphical passwords. The results indicate that the recognition-based (*cognometric*) graphical passwords are more memorable than recall-based (*drawmetric*) graphical passwords, but takes more time to login. None of the previously proposed GUIs [4, 5, 6, 7, 8, 9, 10, 12, 15, 16, 19, 20, 21, 22, 23] combines the advantages of both *cognometric* and *drawmetric* systems. The systems proposed in [19] and [8] use signature-based schemes but do not use a 2D grid technology (draw, digitize and store the signature), and hence are difficult to recall. The system proposed in [12] uses a 2D grid technology but is not a signature-based scheme. Therefore we do not categorize these three [8, 12, 19] as both *cognometric* and *drawmetric* systems.

Handwritten signatures have long been used as a proof of authorship. In general, signatures are authentic, unforgeable, not reusable, unalterable and unrepudiable [19]. Signatures personify a person and are easier to recall than other drawings when drawn on a 2D grid. Therefore we can categorize such signatures as recall-based graphical passwords that have the same or close enough memorability as recognition-based graphical passwords.

In this paper we propose a new graphical Signature-based User Identification System named SUIS. It is based on a 2D grid technology, that is used to draw, digitize and store the signature for user identification. SUIS is categorized as both a *cognometric* and *drawmetric* system. The 2D grid was first used in *Draw a Secret* [12] for user identification. Our model is different than proposed in [12]:

- We take one cell in a grid, as one pixel in the drawing. This makes it much simpler to implement the model and compare the signature in practice.
- For signature matching, the signature drawn has to follow the same grid cells as the signature stored, independent of the sequence. This increases the usability of the system, but decreases the password space. Increasing the usability here means, since the users do not have to follow the same sequence they can draw and remember more complex signatures. The password space can be increased by increasing the number of grid cells.

Some of the characteristics of SUIS are as follows:

- 1) SUIS is easier and faster to compare for signature matching.
- 2) SUIS takes into consideration the angular changes at a coarse level.
- 3) SUIS, by using a digitization technique, provides extra security and protection on top of encryption.
- 4) The signature window i.e; the grid area (number of grid cells) in SUIS can be increased to increase the password space (2^n where n = number of grid cells) of the system. The size of an average grid (extended) used in our empirical study is 7×7 for which the password space is $2^{49} > 10 \times 10^{14}$. The password space for a text-based user identification system for 8 characters (average size) password is $95^{10} > 6 \times 10^{15}$. There are 95 possible character sets including space.
- 5) SUIS is rigorous enough to be a password system, but easy enough to be usable.
- 6) Precision of the signature in SUIS can be changed by decreasing the size of the grid cell of the system. For example, a signature drawn with mouse/finger needs less precision, whereas a signature drawn with pen or other such pointing devices needs more precision.
- 7) SUIS is independent of the language and the device used to write/draw the signature, but is more suitable for touch-based systems (the empirical study presented in this paper was performed on a touch-based system), such as, mobile devices and laptops.
- 8) SUIS is efficient and suitable to be used for online (verification is performed immediately after a password is submitted) authentication systems. Our system is not based on any machine learning model as used in [8]. A machine learning model is not suitable and practical to be used for identifying a user for online authentication systems. Moreover, for successful signature matching such a model needs a large set of training data, i.e; the forged samples of the signatures.

The remainder of the paper is organized as follows. Section II describes and compares research efforts that are similar to SUIS. Section III describes SUIS in detail. We conclude in Section IV.

II. RELATED WORKS

This section discusses some of the previous research efforts on GUIs that are similar to the system proposed in this paper. A thorough survey of these and other systems referenced in Section I can be found in [1, 18].

Syukri et al. [19] proposed a system that uses signatures drawn with mouse for identifying a user. Through experimental evaluation they selected parameters for signature verification and matching. User verification threshold was set to 70%. The size of the signature window was set to 1024×512 pixels. The distance threshold was set to 50 pixels. The parameters selected for signature verification were: (1) Number of signature points. (2) Coordinate of signature points. (3) Signature writing time. (4) Signature writing velocity. (5) Signature writing acceleration.

Experiments were carried out with 21 users. The successful rate achieved was 93%. To calculate the acceleration they used the classical physics formula $a = \frac{F}{m}$, where F is the user's force to push the mouse and m is the mass of the mouse. Although, the number of participants in the experiments carried out in [19] were small to make any definite conclusion, the successful rate reported is very encouraging, and indicates that some of the parameters can be used for a successful signature matching.

SUIS indirectly uses the signature points as part of the grid cells. We do not use the last three parameters selected by [19], as we believe these are not the true representation of a user drawing a signature. In practice the last three parameters are more dependent than the first two parameters, on different environments, such as the mood of the user (e.g; in sickness, sadness and excitement etc), times of the day or night, etc, and hence can produce more true negatives.

Jermyn et al. [12] proposed a system called *Draw a Secret* (DAS), that allows the user to draw a unique password. The password is drawn on a 2D grid. If the stored and the drawn password touches the same grid cells in the same sequence, then the user is authenticated. It becomes difficult to authenticate if the strokes of the user are too close to the grid lines. In this case either, the user is presented with the internal representation to confirm if the cells were actually touched by the drawing, or, the system does not accept a drawing that is too close to a grid line.

As passwords depend on users, the proposed system in [12] lacks an empirical study for its usability. It has only been tested through paper prototypes. Because of lack of a suitable user study we cannot comment on its effectiveness as a GUI.

Everitt et al. [8] proposed a neural network-based system using graphical signatures. The system use a hybrid approach, using both text and graphical passwords. The input devices used are mouse for graphical-based password and keyboard for text-based password. The authenticity of a user is confirmed by the typing style and the signature match. For the typing style they measure two times, one is the time between the two key presses, and the other is the time a key is held down. This idea for the key metrics is similar in concept to the one used in [19] for the mouse metrics. For matching two graphical signatures they use the signature traces, and measure the change in angles and euclidean distances in the two signatures.

The experiments were carried out with 41 participants between the ages of 20 and 30. The results show that they achieved a false accept rate (FAR) of 4.4% and a range of false reject rate (FRR) from 0.2% – 38.6%. FAR is the rate at which forged samples are accepted as genuine and FRR is the rate at which genuine samples are rejected as forgeries.

The system [8] is based on a machine learning model and hence needs training in addition to registration and verification. The training data is usually created by asking users to provide a set of forged signature samples for other users or these forged signature samples are generated automatically. We think this is one of the major problems of using a machine learning model in such systems.

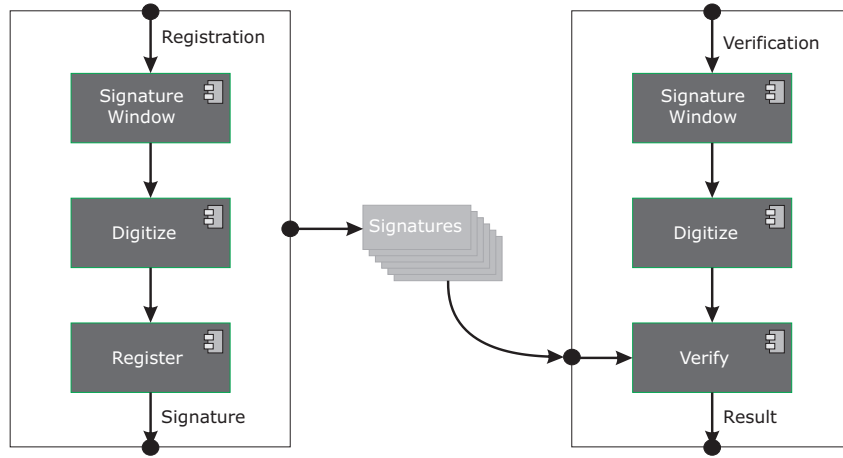


Fig. 1. High level overview of SUIS (Signature-Based User Identification System).

III. SUIS (SIGNATURE-BASED USER IDENTIFICATION SYSTEM)

Figure 1 gives an overview of SUIS proposed in this paper. SUIS has two phases. In the first phase the user registers her/his signature. This signature, after digitizing¹, is stored in the database. In the second phase the signature drawn by the user, after digitizing, is verified against the stored signatures. In case of a match the user is identified as a legal user.

A. The Digitization Technique

We use a simple but practical digitization technique to store the signature. This makes the signature easy to store and compare, but difficult enough to make its extraction non-trivial.

In SUIS, size (number of grid cells) of the 2D grid for drawing the signature range from 25 (5×5) – 49 (7×7), to keep the password space in the range of more than ten million ($2^{25} > 1 \times 10^7$) to more than a trillion ($2^{49} > 1 \times 10^{14}$). Each cell in the 2D grid is stored as part of the signature. There are two grids: the *drawing grid*, that is visible to the user for drawing, and the *extended grid* that includes the *drawing grid* and extra cells, and is used to digitize and store the signature. If a cell in a *drawing grid* contains a drawing, i.e., the pixels touched in the cell are inside the drawing area of the cell, it is stored as 1, otherwise it is stored as 0. To produce a coarser signature, we keep the drawing area in a cell smaller than the area of the cell. The extra cells in the *extended grid* is used to store the value of the color selected by the user and the value of the randomly selected storing technique used. The ability of selecting a color and choosing a random value for the storing technique for the signature also increase the password space.

The user can select a color to draw the signature. To elude shoulder surfing upto an extent, a different value of the color relative to the color selected (in which the signature drawn is displayed) is selected and stored. Shoulder surfing is a technique where a person looks over someone's shoulder to

get information, such as passwords, PINs, other security codes and data. Each color in SUIS is assigned a number. The value of color stored is computed as follows: $color\ stored = number\ assigned\ to\ the\ selected\ color + \lceil \frac{N}{t} \rceil$, where N is the number of total colors used in the system, t is the randomly selected storing technique used and N is $\geq t$. To provide more resistance for shoulder surfing, we erase the signature as soon as it's drawn completely and the user submits it for verification.

We use a number of different techniques for storing a signature. To make the extraction of the information about a signature (grid cells drawn, value of color and storing technique) non-trivial, each time a signature is stored a different storing technique is selected randomly. This information is stored as part of the signature, and also as part of the user's profile, so that during the verification phase of the user the same storing technique is used to verify the signature. Each time, when a user login, a different technique can be used and stored in the user's profile to increase the protection of the user's signature. We also encrypt the signature before storing it. Therefore, this digitization of the signature provides extra security and protection on top of encryption.

B. Signature Storing Techniques

A signature is stored as a 2D matrix. Each cell in the matrix contains either a value 1 or a value 0. Initially all the cells in the matrix contains a value 0. The signature drawn by the user is stored in the cells of the matrix corresponding to the *drawing grid*, as explained above. The *extended grid* contains twice (to take care of $\lceil \frac{N}{t} \rceil$) as many extra cells as the total number of colors that can be used to draw the signature. Based on the value of the color selected, the corresponding cell out of these cells of the matrix gets the value of 1. Similarly the *extended grid* contains another set of additional cells equal to the number of the storing techniques available. Based on the storing technique used, the corresponding cell out of these additional cells of the matrix gets the value of 1.

¹Digitizing also includes encryption. We do not discuss it in this paper because there is already a lot of literature available on encryption.

Each signature's storing technique is given a number (a value) that is stored in the signature, as explained above. We introduce *simple* – *complex* changes in each signature technique to make it different than the other. Some of the changes introduced are:

- 1) Changing the numbering of the signature's matrix (from left-right to right-left and so on).
- 2) Changing the location (start, middle or the end) where the value of the color is stored in the signature's matrix.
- 3) Changing the location (start, middle or the end) where the value of the storing technique used is stored in the signature's matrix.
- 4) Instead of storing a 1 with 0's, we could just store the value of the color and the value of the storing technique in the matrix.
- 5) By splitting or merging the grid cells and storing them at different locations in the signature's matrix.
- 6) By just storing the information about either 0's, 1's or both in the signature's matrix. For example storing only the location of all the 1's in the matrix.
- 7) Combination of two or more of the above techniques.

Other complex storing techniques can also be used to increase protection, such as matrix manipulations, etc, and we leave this to the reader. Using different number of storing techniques gives SUIS the ability to randomize the value of the storing technique, each time a signature is stored, that makes it non-trivial to extract the signature information.

C. Example

We explain the digitization technique described in Section III-A and how it is used for storing (using one of the randomly selected storing techniques) and matching a signature, using an example shown in Figure 2.

A 2D grid of 8×5 is used in Figure 2 for drawing, called the *drawing grid*. The same 2D grid is extended to 10×6 to store the signature, called the *extended grid*. Whenever the signature touches a grid cell, a value of 1 is stored in that grid cell. We store a value of 0 in the grid cell at column 3 and row 5 (shown in *lightgray* color), because the number of pixels touched in the grid cell are less than a predefined threshold value for this grid.

The user, used color *green* to draw the signature and the storing technique (randomly selected) used for storing the signature is numbered 1. So we store number 7 (assuming color *green* = 1 and color *white* = 7, $1 + \lceil \frac{16}{3} \rceil = 7$) and 1 in the *extended grid*, at the end of the matrix (the last 2 columns and the last row). For storing the color number 7, we store a 1 at the corresponding cell, at column 9 and row 4, in the matrix. For this example we have assumed there are 4 signature storing techniques available in SUIS, so the *extended grid* has $16 + 4 = 20$ extra cells. For storing the signature's storing technique number 1, we store a 1 at the corresponding cell, at column 7 and row 6, in the matrix, and the same number is also stored as part of the user's profile.

For matching a signature, we exactly match all the extra cells added to the *extended grid* of all the stored signatures

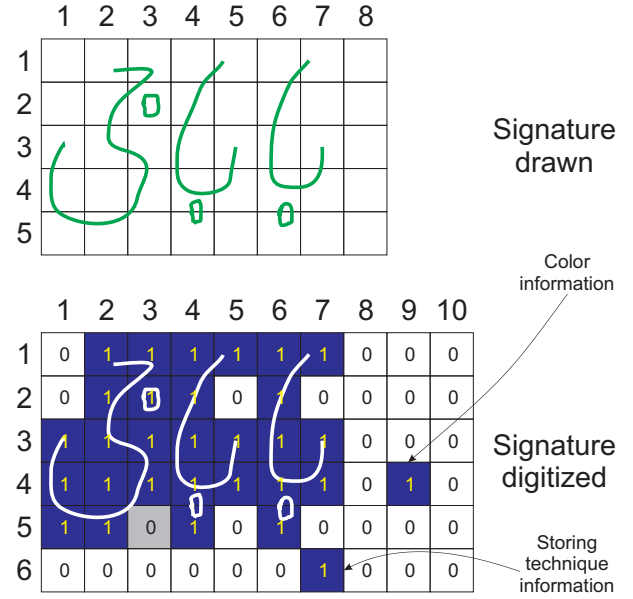


Fig. 2. An example of digitization technique used in SUIS. The signature *Babajee* (as pronounced in English language), a word used in Urdu and Hindi languages to refer an old man with respect, is digitized.

with all the extra cells added to the *extended grid* of the signature drawn for the verification. In case of a successful match we match the corresponding *drawing grid* of the stored signature with the *drawing grid* of the signature drawn for the verification, based on a predefined threshold value for the grid. If the difference is \geq to the predefined threshold value the match is successful, and the user is verified as a legal user.

IV. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a new graphical signature-based user identification system, that is efficient and practical to be used in login systems. The system is rigorous enough to be a password, but easy enough to be usable. It is independent of the language used to write/draw the signature.

Currently we are developing a prototype tool in Java to implement SUIS. In future we will carry out a study with a large number of participants and evaluate the validity of SUIS using a number of metrics, such as *Usability*, *Deployability* and *Security* described in [3]. To improve the usability of the current technique, in future, we will develop different techniques, such as by integrating joining blocks/lines that will make it easier to form a shape or a drawing as a graphical signature, etc, and test the pros and cons of each such technique through a large scale empirical study.

REFERENCES

- [1] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. Graphical Passwords: Learning from the First Twelve Years. *ACM Comput. Surv.*, 44(4):19:1–19:41, September 2012.
- [2] Greg E Blonder. Graphical Password, September 24 1996. URL <http://www.google.com/patents/US5559961>. US Patent 5,559,961.

- [3] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 553–567. IEEE, 2012.
- [4] Microsoft Corporation. *Windows 8 Picture Password*, Last accessed: May 31, 2016. URL <http://windows.microsoft.com/en-ca/windows-8/personalize-pc-tutorial>.
- [5] Passfaces Corporation. *The science behind Passfaces, White paper*, Last accessed: May 31, 2016. URL http://www.passfaces.com/enterprise/resources/white_papers.htm.
- [6] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems. *Int. J. Hum.-Comput. Stud.*, 63(1-2): 128–152, July 2005.
- [7] Paul Dunphy and Jeff Yan. Do background images improve “draw a secret” graphical passwords? In *Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS ’07*, pages 36–47, New York, NY, USA, 2007. ACM.
- [8] Ross A. J. Everitt and Peter W. McOwan. Java-Based Internet Biometric Authentication System. *IEEE Trans. Pattern Anal. Mach. Intell.*, 25(9):1166–1172, September 2003.
- [9] Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu. YAGP: Yet Another Graphical Password Strategy. In *Proceedings of the 2008 Annual Computer Security Applications Conference, ACSAC ’08*, pages 121–129, Washington, DC, USA, 2008. IEEE Computer Society.
- [10] Naveen Sundar Govindarajulu and Sriganesh Madhvanath. Password Management Using Doodles. In *Proceedings of the 9th International Conference on Multimodal Interfaces, ICMI ’07*, pages 236–239, New York, NY, USA, 2007. ACM.
- [11] E.L. Holt, M.E. Kowalczyk, and R. Humphries. Image or pictographic based computer login systems and methods, January 21 2014. URL <http://www.google.com/patents/USRE44725>. US Patent RE44,725.
- [12] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. The Design and Analysis of Graphical Passwords. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8, SSYM’99*, pages 1–1, Berkeley, CA, USA, 1999. USENIX Association.
- [13] Valerie S. Nelson, Douglas L. Reed and John R. Walling. Pictorial Superiority Effect. *Journal of Experimental Psychology: Human Learning and Memory*, 2(5):523–528, 1976. ISSN 0033-3131.
- [14] Allan Paivio, T.B. Rogers, and PadricC. Smythe. Why are pictures easier to recall than words? *Psychonomic Science*, 11(4):137–138, 1968. ISSN 0033-3131.
- [15] Google Play. *Lock Screen Pattern*, Last accessed: May 31, 2016. URL <https://play.google.com>.
- [16] SFR Software. *visKey for Pocket PC*, Last accessed: May 31, 2016. URL <http://www.sfr-software.de/cms/EN/pocketpc/viskey>.
- [17] Elizabeth Stobert and Robert Biddle. Memory Retrieval and Graphical Passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS ’13*, pages 15:1–15:14, New York, NY, USA, 2013. ACM.
- [18] Xiaoyuan Suo, Ying Zhu, and G. Scott. Owen. Graphical Passwords: A Survey. In *Proceedings of the 21st Annual Computer Security Applications Conference, ACSAC ’05*, pages 463–472, Washington, DC, USA, 2005. IEEE Computer Society.
- [19] AgusFanar Syukri, Eiji Okamoto, and Masahiro Mambo. A user identification system using signature written with mouse. In Colin Boyd and Ed Dawson, editors, *Information Security and Privacy*, volume 1438 of *Lecture Notes in Computer Science*, pages 403–414. Springer Berlin Heidelberg, 1998.
- [20] Tafasa. *Patternlock*, Last accessed: May 31, 2016. URL <http://www.tafasa.com/patternlock.html>.
- [21] H. Tao and C. Adams. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. *International Journal of Network Security*, 7(2):273–292, 2008.
- [22] GrIDSure Corporate Website. *GrIDSure*, Last accessed: May 31, 2016. URL <http://www.gridsure.com>.
- [23] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *Int. J. Hum.-Comput. Stud.*, 63(1-2):102–127, July 2005.